IEEE 802.11s Experimental Evaluation at WIDE Camp

[†]Muhammad Imran Tariq, [‡]Shoichi Sakane, [†]Yoichi Shinoda
[†]Dependable Network Innovation Center
Japan Advanced Institute of Science and Technology, Ishikawa Japan
{imran, shinoda}@jaist.ac.jp
[‡]Cisco Systems, Tokyo Japan
ssakane@cisco.com

Abstract
The IEEE 802.11s standard is emerging with rich set of features to improve the performance of wireless mesh networks (WMNs) and extend the coverage of access networks. The main distinctiveness of this standard is multihop frame forwarding at MAC layer: HWMP (Hybrid Wireless Mesh Protocol) is defined as default path selection protocol, besides it ALM (Airtime Link Metric) is proposed as path selection framework/routing metric. This study presents an evaluation of IEEE 802.11s based network which was deployed at WIDE camp with intention to providing a MBBS (Mesh Basic Service Set). To examine the performance of HWMP and ALM in this real deployment, both TCP and UDP traffic flows were supported. The interworking and multiple addressing schemes are discussed in this study with challenging research issues those involved in performance degradation.

Keywords: *IEEE 802.11s, HWMP, ALM, MBBS, real time traffic*

Introduction

The IEEE 802.11 WLANs, basic service sets (BSSs) are playing a key role to provide internet access via Ethernet LANs. The wireless network deployment increases the cost when its coverage is extended and reduces flexibility due to immobility and fixed backbone architecture [1]. The IEEE 802.11 standard also defines independent basic service set (IBSS) as wireless ad hoc networking. Moreover in this mode, communication is taken place among stations (STAs) without access points (APs) and distribution system (DS). Consequently, it has been realized that independent infrastructure is not sufficient for internet access and for the support of BSSs. Therefore, the amalgamation of BSSs and IBSS has become the research challenge for researcher and urge to revisit the design of networking protocols.

Due to their self-organization, self-management and self-healing traits, WMNs have emerged a next generation wireless technology to provide better services and address the realized requirements [2]. But the dissimilarities among proprietary solutions make the deployment of WMNs impractical and increase the interoperable complexities. To address these issues, IEEE 802.11s task group has been established and IEEE 802.11s standard is almost waiting to be public. The IEEE 802.11s is being considered a promising solution for WMN with MAC layer path selection framework. In this standard, WMN is formed by mesh STAs to provide mesh facility that is also called mesh backbone or mesh BSS (MBSS), mesh STAs establish peer-to-peer links and transfer messages mutually [3]. As it is shown in Fig. 1 mesh STAs do not communicate with non mesh STAs but MBSS might also be linked with distribution system. To do it, a logical architectural component is introduced that is called mesh gate (MG) to integrate/interconnect the mesh BSS with other BSSs through the DS. Communication occurs between MBSS and DS via one or more mesh gates; it means MSDUs from an MBSS enter to IEEE 802.11 DS at theses logical points. Whereby, MBSS can also be integrated with non IEEE 802.11 LAN. To incorporate the IEEE 802.11 DS that these mesh BSS associate to, the DS should contain the portal. As a result, mesh gate and portal are different component because portal integrates the IEEE 802.11 architecture with non IEEE 802.11 LAN; mesh gate integrates the MBSS with IEEE 802.11 DS. The mesh STAs may also be collocated with APs to play double role such as mesh STA and AP, consequently new entity with the name MAP is formed that provides services to infrastructure BSS.

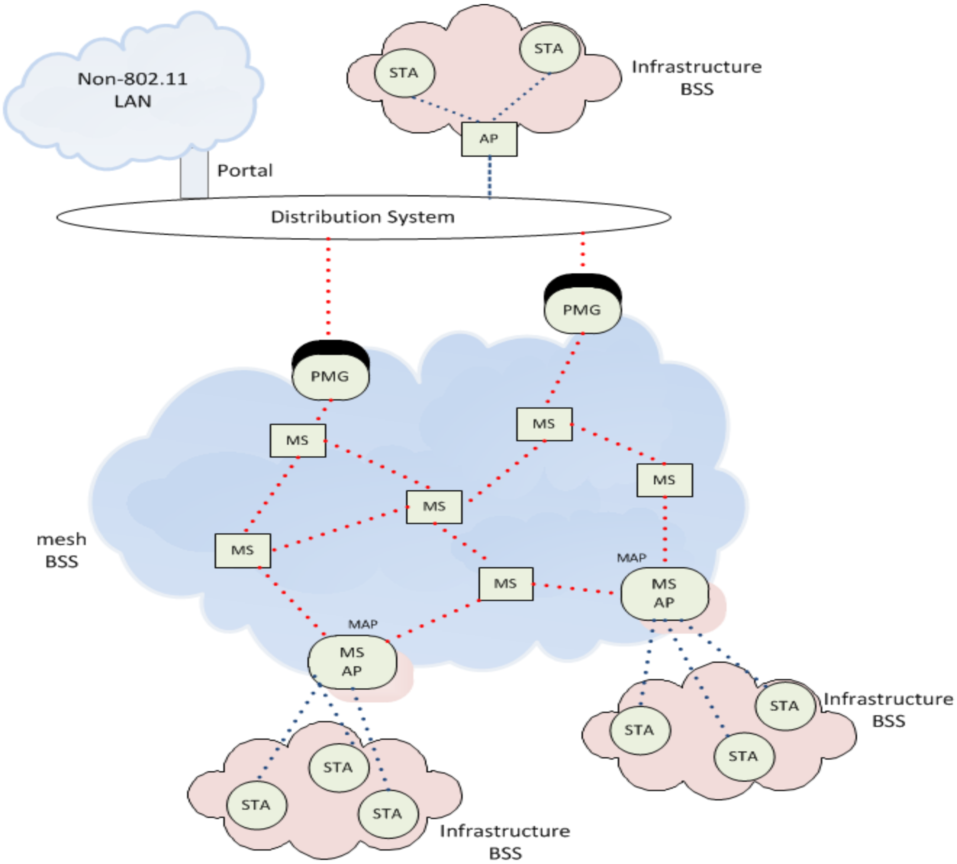


Figure.1. IEEE 802.11s architecture representing MS, PMG, MAP, Portal, DS

This WMN may gain significant attention and can be promising candidate for rich set of applications e.g. broadband home networking, wireless enterprise networks, community based networking, building automation and wireless broadband services [4]. Especially, delivering Internet access to the last leg is one of the most promising applications as can be seen in Fig. 1 seemingly integration of WMN with IEEE 802.11 DS and non IEEE 802.11 LAN immensely reduces the deployment cost and increases coverage area. One of the unique characteristics of IEEE 802.11s is the implementation of mesh path selection and multi hop forwarding at link level. The HWMP and ALM are introduced as default routing protocol and link quality metrics respectively. The goal of this study is to investigate the performance of real deployment of IEEE 802.11s WMN publically. To estimates the performance of WMN, we mainly focus on path selection framework with different configuration parameters. The results point out the challenging issues that degrade the performance of publically deployed IEEE 802.11s network. Based on this evaluation, we provide the feedback to enhance the performance that should be considered for network deployment especially at public places.

This document is organized as follows: Section 2 contains the detail of path selection framework and features of IEEE 802.11s. Configurations of network deployment and its topology is presented in section 3. The results and discuss is described in section 4. Section 5 is concluded with concluding remarks.

Path Selection Framework and Features of IEEE 802.11s

In September 2003, IEEE initially formed a study group for adding IEEE 802.11s network in IEEE 802.11 standard, then on July 2004 the study group was reformed and it became the Task Group. The first draft was issued on March 2006 by the TG and several others were also issued onward. Even though by the time of writing this document the standard is not finalized yet, last meeting of the TG was held on July 2011 and the draft approved by EC and has been forwarded to REVCOM to be standardized [5]. The IEEE 802.11s standard has defined the set of services that is called mesh services which are provided by the following mesh facilities: 1. Mesh discovery, 2. Mesh peering management, 3. Mesh security, 4. Mesh beaconing and synchronization, 5. Mesh coordinate function, 6. Mesh power management, 7. Mesh channel switching, 8. Three address, four address and extended address frame format, 9. Mesh path selection and forwarding, 10. Interworking with external networks, 11. Intra-mesh congestion control, 12. Emergency service support in mesh BSS. The detail of following mesh facilities can be found in [3].

1. **Mesh discovery**
   In order to find out a functioning mesh BSS, the mesh STAs perform either active scanning or passive scanning. A mesh profile that defines the configuration parameters of the mesh BSS, is also acquired through this scanning process. A mesh profile comprises on Mesh ID, path selection protocol and metric, congestion control mode, synchronization method and

authentication method. These elements help to determine the mesh active profile for the scanning mesh STA. Based on the scanning results, mesh STA becomes the member of functioning mesh BSS or initiates the new mesh BSS.

2. **Mesh peering management (MPM)**

   A mesh STA that is accepted as a member of an MBSS establishes a mesh peering using mesh peering management (MPM) protocol with one or more neighbor mesh STAs those are in the same MBSS. The mesh peering management protocol establishes, maintains and closes mesh peerings between mesh STAs. While peering with correspondent STA, MPM exchanges different kind of frames e.g. Mesh Peering Open frames, Mesh Peering Confirm frames, and Mesh Peering Close frames. To perform a successfully mesh peering following requirements must be satisfied 1) both mesh STAs have correctly exchanged a Mesh Peering Open frame for potential mesh peering; 2) both mesh STAs have correctly exchanged a Mesh Peering Confirm frame for this peering.

3. **Mesh security**

   The mesh peering could be secured and depends on the mesh link security protocols. The used mesh authentication protocol authenticates a pair of mesh STAs and establishes shared common pairwise master key (PMK) between them. The authenticated mesh peering exchange (AMPE) mechanism trusts on the presence of the PMK between the two mesh STAs to establish an authenticated peering and derive session keys.

4. **Mesh Beaconing and synchronization**

   All mesh STAs periodically transmit Beacon frames that are specific to an MBSS with the purpose of assisting mesh discovery, mesh power management, and synchronization processes. The IEEE 802.11s also defines mesh beacon collision avoidance (MBCA) protocol to detect and mitigate collision among even two hop neighbors Beacon frames.

   The IEEE 802.11s standard introduces neighbor offset synchronization method as the default and mandatory synchronization method. The purpose of this method is enable minimal synchronization capabilities and interoperability between mesh STAs that use MCCA, MBCA, or operate in light or deep sleep mode. The standard also defines an extensible framework to facilitate the support of multiple synchronization methods for mesh STAs.

5. **Mesh coordinate function (MCF)**

   The mesh STA uses MCF for channel access. MCF comprises on two channel methods, EDCA and MCCA. These methods are accessed through two types of transmission opportunities (TXOP) which are basic unit of allocation of the right to transmit onto WM, using MCF: EDCA TXOP and MCCA TXOP. Each TXOP is described by starting time and a defined maximum length. The EDCA TXOP is assigned to a mesh STA who wins an instance of EDCA contention. The MCCA TXOP is assigned to a mesh STA who gains control of the WM during an MCCAOP. The MCCAOP is defined as an interval of time for frame transmission that has been reserved by means of the exchange of MCCA frames.

6. **Mesh power management**

   The standard introduces three types of power modes to reduce power consumption. A mesh STA sets the power mode of each its mesh peering either active, light sleep, deep sleep mode. A mesh STA also maintains mesh awaken window when it is either in light sleep mode or in deep sleep mode. A mesh STA has the capability to buffer frames and perform mesh power mode tracking for the peer-specific mesh power modes of its peer mesh STAs. A mesh STA also supports the capabilities for individually or group addressed frame transmissions to neighbor peer mesh STAs that are either in light sleeping mode or deep sleeping mode.

7. **Mesh channel switching**

   A channel switching protocol is defined to avoid interference or to reassign mesh STA's channels to ensure the MBSS connectivity. A mesh informs each of the peer mesh STAs using Channel Switch Announcement elements together with Mesh Channel Switch Parameters element in Beacon frames, Probe Response frames, and Channel Switch Announcement frames that the mesh STA moving to a new channel. The "Selecting and advertising a new channel" protocol is introduced to propagate a channel switch throughout whole MBSS including mesh STAs in power mode. The mesh STA is also capable to operate in multiple regulatory classes. A Channel switch across a regulatory class protocol is defined to assist on multiple classes.

8. **Frame addressing in an MBSS**

   The multiple frame addressing enables Mesh Data frames and Multihop Action frame forwarding in an MBSS using Mesh Control field. Three kinds of frame addressing for Mesh Data are introduced, these are as following: three addresses (mesh data group addressed), four addressed (Mesh Data individually addressed, Mesh Data proxied group addressed), and six addressed (Mesh proxied individually addressed). Like Mesh Data addressing schemes, there are two frame addressing introduced as following: three addresses (Multihop Action group addressed), and Multihop Action individually addressed. These addressing methods help to forward packet within a MBSS or from infrastructure BSS to ESS.

9. **Mesh path selection and forwarding**

   The IEEE 802.11s introduces a mesh path selection framework to enable path discovery over multiple instances of WM within a mesh BSS at link layer. It also supports an extensible framework that might be used to support specific routing protocol or metric. Mesh path selection framework is divided into two parts as following

   - Mesh path selection protocol
   - Mesh path selection metric

   a) **Mesh path selection protocol**

The hybrid wireless mesh protocol (HWMP) is a default/mandatory path selection protocol and due to its flexibility can be operated in on-demand path selection with proactively tree topology. It uses common set of protocol elements, generation and processing rules inspired by AODV and adapted for MAC address-based path selection and link awareness metric. HWMP can be configured in two modes of operation; each of them provides different level of functionality.

i. *On-demand mode*

In this mode mesh STA initiates path request to a destination node using PREQ broadcast frame with specified destination address and metric initialization which is zero in the beginning. When a mesh STA receives a PREQ it creates or updates its path information to originator node if HWMP sequence number is greater than current path or HWMP sequence number is same but path metric is better than current path. The mesh STA broadcasts it again to its peer mesh STAs. Whenever mesh STA broadcasts a PREQ it updates the metric in PREQ field to reflect the cumulative metric of the path to the originator mesh STA. Upon receiving a PREQ, target mesh STA creates or updates path to the originator mesh STA and individually reply back with PREP frame. Intermediate nodes in an MBSS receives PREP frame and create/update path to the target mesh STA and forward frame to the originator.

ii. *Proactive tree building mode*

There are two mechanisms available to successfully disseminate information for reaching root mesh STA.

- Proactive PREQ mechanism

  Tree building process begins with sending PREQ element by root mesh STA with target address set to all one and TO field 1. The PREQ element sent periodically by mesh root STA and contains the path metric initial value of the active path selection metric and increasing HWMP sequence number. Remaining whole process is repeated similar to on-demand mode.

- Proactive RANN mechanism

  The root mesh STA periodically propagates a RANN element in an MBSS. The information contained in the RANN is used to disseminate path metrics to the root mesh STA, but reception of a RANN does not establish a path. Upon reception of a RANN, each mesh STA has to create or refresh a path to the root mesh STA and sends an individually addressed PREQ to the root mesh STA via the mesh STA from which it received the RANN. The root mesh STA sends PREP in response to each PREQ. The individually addressed PREQ creates the reverse path from the root mesh STA to the originator mesh STA, while the PREP creates the forward path from the mesh STA to the root mesh STA.

b) **Mesh path selection metric**

The IEEE 802.11s standard defines ALM as a default link metric that is used by path selection protocol to identify an efficient radio-aware path. Due to framework extensibility this metric can be replaced by any path selection metric as specified in the mesh profile. As it is a radio-aware metric, it reflects the amount of channel resources consumed by transmitting a frame of specific size over a particular link. Airtime for each link is computed as follows:

$$C_a = \left[O + \frac{B_t}{r}\right] \frac{1}{1 - e_f}$$

Where *O* and Bt are constants quantifying the Channel access overhead (including frame headers, training sequences, access protocol frames, etc.) and the number of bits in a probe frame. The rate *r* represents the transmission rate in Mb/s for a frame of standard size B_t and its assessment is dependent on local implementation of rate adaptation. The IEEE 802.11s specifies the frame error rate e_f as the probability of standard size B_t frame corrupted due to transmission error which is transmitted at the current transmission bit rate *r*.

Mesh forwarding framework is referred to forwarding MSDUs and MPDUs on selected paths between mesh STAs at link layer. The mesh paths are contained in the forwarding information as table. The forwarding information also indicates the lifetime of the paths. The detail of mesh forwarding can be found in section 8.

10. Interworking with DS

As illustrated in Fig. 1 an MBSS might have interaction with distribution system to forward packet/receive from, through one or more mesh gates. The gate announcement is done by two ways, either it is done by sending Gate Announcement frames or alternatively HWMP path selection frames using Root Announcement element frame or Path Request element frame, when it configured as root mesh STA. The advantage of Gate Announcement is to select an appropriate mesh gate and build a path toward it. The mesh gate becomes proxy mesh gate when it has access to IEEE 802 STA outside an MBSS. A proxy mesh gate has the addresses knowledge of the other proxy mesh gates in the MBSS and of external addresses proxied by them through the receipt of path selection messages and messages carrying proxy information.

11. Intra-mesh congestion control

The standard provides three kinds of intra-mesh congestion control mechanisms to control flow over multihop-communication: local congestion monitoring and congestion detection, congestion control signaling, and local rate control. Intra-mesh congestion control mechanism is useful to mitigate the wasteful utilization of WM caused by buffer overflow at mesh STA. This standard specifies the congestion control signaling protocol as default and available in any MBSS, it also allows the inclusion of more advanced congestion control schemes.

12. Emergency service support in an MBSS

The support of emergency services might be authorized over IEEE 802.11s network. In order to support emergency services in mesh networks the Beacon and Response frames are used to inform and advertise to peering mesh STAs that mesh STA supports emergency services. In case of emergency services required to a mesh STA, an emergency indication bit is set within the Mesh Peering Open frame. Mesh STAs that support emergency services, accept peering from other mesh STAs requiring emergency services, transferring frames to an emergency server.

Network Configuration and Experimental Topology

We set up mesh basic service set (MBSS) for the purpose of providing mesh facility to collocated infrastructure BSS at WIDE camp. We also went through in this mesh network for few experiments with the intention to validate the implemented path selection framework. In the following section we discuss about the deployed topology, devices and configuration parameters.

1. Deployed topology

A simple MBSS was deployed to provide backhaul network to legacy 802.11 user stations, i.e. non-mesh devices. Used network topology described in Fig.2 contains one wireless router as mesh gate (Mesh Gate) and 10 wireless routers as mesh STAs, all mesh STAs are collocated with APs. The big/WS hall was used for different kind of WS (Workshops) and two routers one hope away were deployed there to extend the backhaul network.

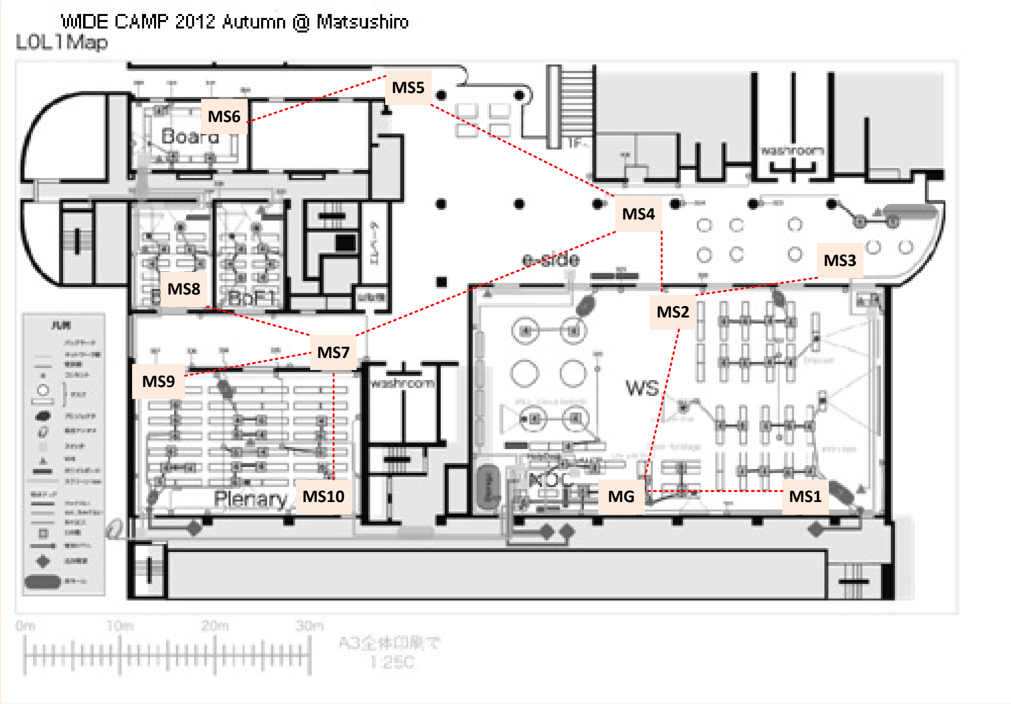


Figure.2. Deployed network topology at WIDE camp

One router at smoking area and other one near to coffee area were deployed and they represent two hop network. The router 6 was deployed in the board meeting room which is a dedicated room for board members and beside it router 5 was also deployed as rely/forwarder, so it becomes 4 hops network. The mesh router 8, 9, and 10 were installed in the plenary and BoF rooms that were used for plenary and BoF sessions, to forward the traffic of them router 7 which was acting both as AP and traffic forwarder was placed near to these room. Thus it was representing three and four hops network. The covered places and the number of maximum attendees are presented in table 1. We are unable to report the exact number of participant but each room was almost full during the meeting time. Each room was divided by thick walls and all doors were closed expect the WS room.

Table I: Illustrates the rooms' capacity at WIDE camp [6].

Room Name	People Capacity
Workshop (WS)	200 people (*1015m2*)
Plenary	150 (*175m2*)
BoF	60 (*less than 100m2)*
Board	20 (*less than 100m2*)

2. **Devices**

The mesh backhaul network was built using Buffalo WZR-HP-AG300H dual band wireless devices that are considered high power and compatible with manifold standards [7]. The open-source firmware OpenWrt with revision r33270 and Linux kernel series 3.0, please refer to [8], was installed on these devices for the purpose of constructing layer 2 mesh network. Each device contains two wireless network interface cards (NICs), one wireless card supports *a/n* and second one supports *b/g/n* standards with multirate operations. Besides these, it also has two more ethernet interfaces, one for to communicate with distribution system (DS) and other one for LAN users. All these interfaces can be configured with DHCP server and connected through bridge functionality.

3. **Network setting and configuration**

In this section, we discuss about the network setting/configurations that has been shown in Fig.2. In the mentioned topology, the backhaul network was operated in 802.11g standard with channel 6 while infrastructure BSS was configured on 802.11a standard with channel 40. In order to send/receive packets to and from backhaul network both networks were collocated with bridging functionality. For the purpose of providing IP address leases to legacy 802.11 users, only mesh gate (MG) was configured as DHCP server in the whole network. We configured the backhaul network to closely examine the performance of TCP and UDP traffic along with operations of HWMP and ALM, in both mode reactive mode/topology and proactive mode/topology. The configuration commands with the parameters that were used in establishment of an MBSS are given in appendix1.

Results & Discussion

While experimentation, we have used *iperf* [9] to measure the hop by hop bandwidth of TCP and UDP protocols in the illustrated network topology. Because we also captured the traffic through Tcpdump but due to misconfiguration of parameters, desired evaluation target could not be achieved. Therefore, in this section we are only presenting few results. As fig.3 is showing the hop by hop throughput available in the network.

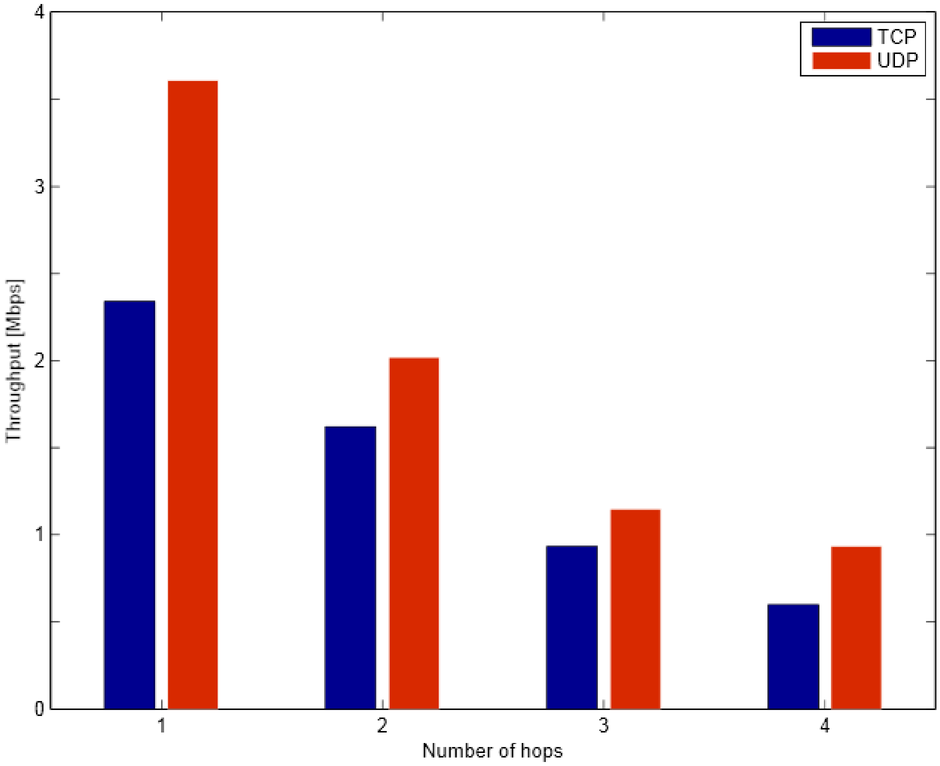


Figure.3. Representing the average network throughput for TCP and UDP against the number of hops

The overall throughput of backhaul network is very less as compare to others evaluation. Besides it, as the number of hops increase the end-to-end throughput decreases respectively. The TCP typically has fewer throughputs than UDP due its acknowledgement traits. Earlier we mentioned, the used firmware lacks of multiple channel switching algorithms support, therefore only single channel was used in this backhaul network. As a result, the overall throughput degradation in this scenario is very well known fact in single-channel single-radio multihop wireless mesh network. The use of single channel in the whole mesh BSS leads to throughput degradation. It has become quite significant challenge for research communities to address this issue with multiple channel switching support. Second reason of throughput degradation is that nodes were deployed in quite human density region, as you know human body is rich with water, so wireless signal can be absorbed at some extend. The interference in this scenario is common not only by peering devices but also from other wireless devices/deployed networks, e.g. smart phones, laptops etc. In the end, routing overhead also can not be ignored because new route calculation which occurs every 5 seconds by default and it takes time to collecting information of the whole network. Based on this information, routing protocol designs/updates routing table. We also noticed, route recalculation event often is trigged before 5 seconds and it is called protocol inability, due it this, packets forwarding process is interrupted and ultimately it plays a role in throughput degradation.

However we captured the metric value of routing protocol for the purpose to show, how much the links are healthy. Fig.4. Illustrating that the effect of interference sources is also being reflected by ALM calculation/values. Such as the number of hops in the network increase the value is also increases. We have seen ALM's formula before; it heavily depends on frame loss and operating data rates. So, as a result of ALM values it might be supposed that these infer the available system throughput. But there required accurate algorithms to properly calculate the frame loss and date rate. Because wrong paths selection has great impact on throughput, especially in WMNs because they are being designed for backhaul network and they also need to satisfy the requirements of real time applications. We need to remind that methods for the calculation of frame loss and date rates are beyond the scope of this report.

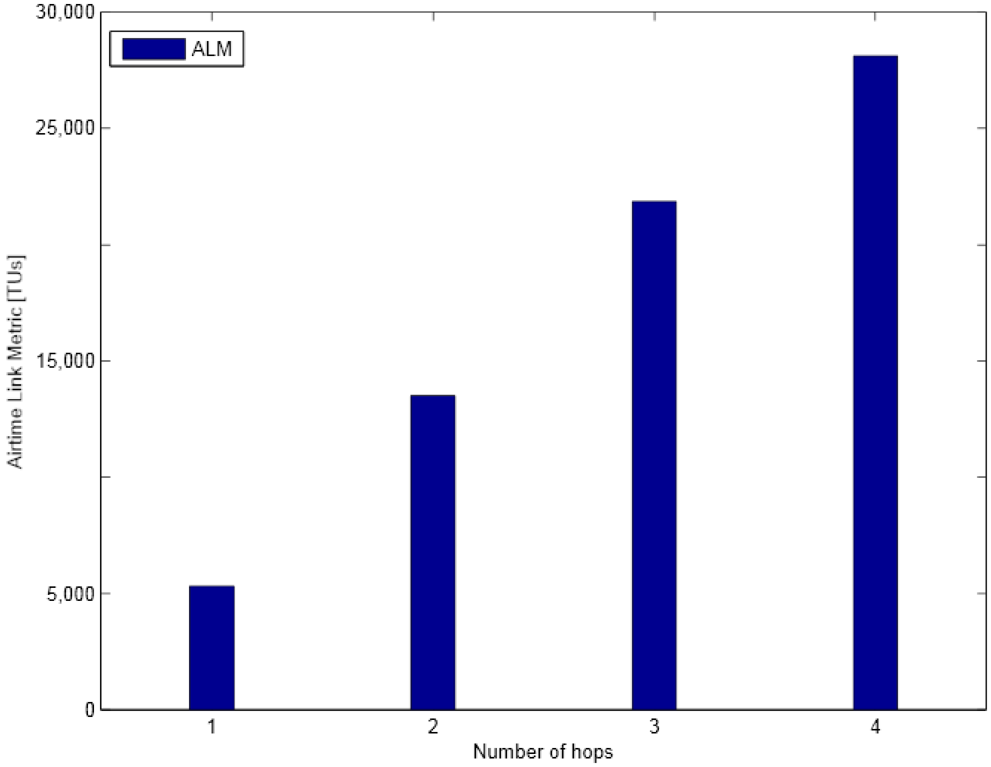


Figure.4. Showing the value of Airtime Link Metric in TUs alongside number of hops

Acknowledgement

We would like to express our gratitude to all those who gave us the possibility to complete this report. We deeply thank to Razvan Beuran, Ken-ichi Chinen, Keiichi Shima and Yuzo Taenaka for providing their support while configuring the network, analyzing the results and reviewing the report.

References

[1] Xudong Wang , Azman O. Lim, IEEE 802.11s wireless mesh networks: Framework and challenges, Ad Hoc Networks, v.6 n.6, p.970-984, August, 2008 [doi>10.1016/j.adhoc.2007.09.003]

[2] I. F. Akyildiz and X. Wang "A Survey on Wireless Mesh Networks", *IEEE Commun. Mag.*, vol. 43, no. 9, pp.S23 -S30, 2005

[3] "IEEE p802.11s/d12.0. draft amendment to standard- IEEE 802.11s: Mesh Networking," May 2011

[4] R. M. Abid, T. Benbrahim, and S. Biaz, “Ieee 802.11s wireless mesh networks for last-mile internet access: An open-source real-world indoor testbed implementation,” *Wireless Sensor Network*, vol. 2, no. 10, pp. 725–738, 2010

[5] The status of ieee 802.11s standard. [Online]. Available http://grouper.ieee.org/groups/802/11/Reports/tgsupdate.htm

[6] The operation report of WiFi mesh network at WIDE camp 2012 spring [Online]. Availabe at https://member.wide.ad.jp/tr/wide-tr-wi-wifi-mesh-camp-1203-00.pdf

[7] http://www.buffalotech.com/products/

[8] https://openwrt.org

[9] https://iperf.sourceforge.net

[10] https://github.com/cozybit/open80211s/wiki/HOWTO-0.4.0

Appendix 1

Wireles mesh network IEEE 802.11s support is availabe from 2.6.26 kernel. You can use latest promoted kernel to deploy mesh network. We suppose, the latest OpenWRT (trunk) firmware with all required and compatabile packages are installed on your devices. Now you intend to build mesh network, for that please follow these given instruction. The detail about these commands can be found in [10].
To configure a network, you have to login the device being root user and need to run the device's terminal.

Setup Mesh Network:

You can have knowledge about how many interfaces your device has by using following command

```
# $ ifconfig
```

Parameters setting of the interfaceses also can be done with it.

The following commands should be installed properly to setup mesh network.

```
# $ iw
```

This command is used to create wireless interface, configuring and changing vaious parameters of it.
To add a mesh interface on specific *wlan* device need to follow the following commands.

```
# $ iw phy phy$i interface add $MESH_IFACE type mp
```

This command creates a mesh interface on user specific device/interface e.g. phy$i with the type MP (Mesh Point, above we have used MS mesh STA as alternative of mp) or it will act as mesh point. The user example of this command is as follow:

```
# $ iw phy phy0 interface add mesh0 type mp
```

Now need to be joined it with existing mesh network or create new mesh network by spcifying the $MESH_ID. This mesh id is used in Beacon frame to recognize the network. The mesh nodes with same mesh id are only able to communicate with each others. It can be done along with above said command or by separate command too.

```
# $ iw phy phy$i interface add $MESH_IFACE type mp meshid $MESH_ID
Or
# iw dev $MESH_IFACE mesh join $MESH_ID
```

To execute this command successfully you need to specify mesh interface ($MESH_IFACE) and mesh id ($MESH_ID) properly and remaining are the default parameters of the command. The user example is as follow:

```
# $ iw phy phy0 interface add mesh0 type mp meshid StarMesh
or
# iw dev mesh0 mesh join StarMesh
```

To make the interface operational, you have to bring the interface up by.

```
# ifconfig $MESH_IFACE up
e.g
#ifconfig mesh0 up
```

Even IP address to this interface can be assigned but it is not necessary depends upon your requirement and deployment scenario. In our design we assigned IP addresses to the interfaces. If you also want then configuration command is executed like.

```
# ifconfig $MESH_IFACE $IP_ADDRESS up
Or e.g
#ifconfig mesh0 192.168.1.1 up
```

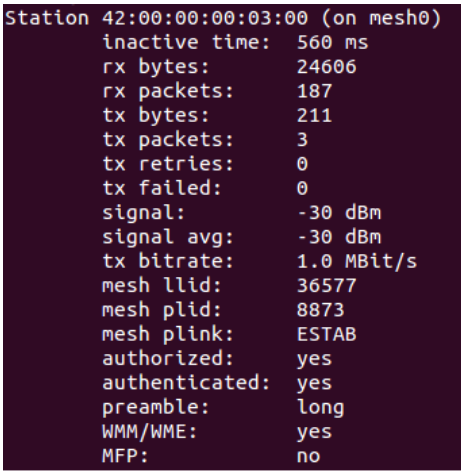
Now time to assign the wireless channel to interface which is decided a common channel for communication. As we have discussed before there is no channel switching mechanism exist. But default channel 1 is assigned to interface. So, if there is plentiful interference on channel 1 then you can assign/switch to another common channel. The channel choice depends on user wish. The following command is used to do it.

```
# iw dev $MESH_IFACE set channel
Or e.g
# iw dev mesh0 set channel 6
```

The MS (Mesh Station) by default contain peering management protocol to establish and maintain the peering with neighbor stations those have same mesh id. In order to have information about peer nodes the following command is used.

```
# iw dev $MESH_IFACE station dump
Or e.g
# iw dev mesh0 station dump
```

The output of this command is listed as



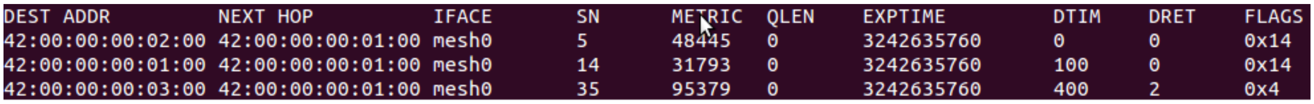
```
Station 42:00:00:00:03:00 (on mesh0)
        inactive time:  560 ms
        rx bytes:       24606
        rx packets:     187
        tx bytes:       211
        tx packets:     3
        tx retries:     0
        tx failed:      0
        signal:         -30 dBm
        signal avg:     -30 dBm
        tx bitrate:     1.0 MBit/s
        mesh llid:      36577
        mesh plid:      8873
        mesh plink:     ESTAB
        authorized:     yes
        authenticated:  yes
        preamble:       long
        WMM/WME:        yes
        MFP:            no
```

The result of that command, displays rich information e.g signal power, tx bitrates, tx retries etc, about peer nodes. As you can see the 13th line (mesh plink: ESTAB) tells us whether it has established peering services with neighbor node or not.

Now you should ping in the network to any node. By doing that and using *iw* command you can have a look on routing table information that reveals where the actually packet is sent in order to get its destination. The following commands show the whole mesh routing table with detail information.

```
# iw dev $MESH_IFACE mpath dump
Or e.g
# iw dev mesh0 mpath dump
```

The output of this command is listed below



```
DEST ADDR         NEXT HOP          IFACE    SN    METRIC  QLEN  EXPTIME     DTIM  DRET  FLAGS
42:00:00:00:02:00 42:00:00:00:01:00 mesh0    5     48445   0     3242635760  0     0     0x14
42:00:00:00:01:00 42:00:00:00:01:00 mesh0    14    31793   0     3242635760  100   0     0x14
42:00:00:00:03:00 42:00:00:00:01:00 mesh0    35    95379   0     3242635760  400   2     0x4
```

The detail of routing table is as follows:

DEST ADDR

The first column represents the MAC address of destination node that can be 1 or more than 1 hop away in the network.

NEXT HOP

Second column indicates the MAC address of next hop for the destination node/address. The first and second columns can be same if destination node is just one hop away or it is peer/neighbor node.

IFACE

The third column tells about the interface who contains this information or where packet is forwarded.

SN

The fourth column is about the PREQ sequence number. It is used to detect and break the loop while path is being investigated.

METRIC

The sixth column contains value for ALM and telling how the path healthy is. This information depends on the number of hops from asked interface to destination interface/address. Therefore each value is different from other destination.

QLEN

This column gives MAC layer queue status at path discovery time.

EXPTIME

The eighth column holds path expiry duration in (TUs) for the given interface to destination interface.

DTIM

This field tells about the buffered broadcast/multicast data on mesh STA. During the mesh DTIM period, the mesh STA transmits broadcast traffic for its neighbors. The mesh STA with power saving capability must switch from doze to awaken state for every DTIM of their peer mesh STAs.

DRET

The column number tenth shows that how many retries have occurred while path from source interface to destination address was being discovered.

FLAGS

The last column contains bit masking type values for different stat flags for paths.